NASA Procedural Requirements

NPR 1600.3
Effective Date: May 31, 2012
Expiration Date: May 31, 2017

COMPLIANCE IS MANDATORY

Personnel Security

Responsible Office: Office of Protective Services

Table of Contents

Chapter 3. Personnel Security Investigations for National Security Positions

Appendix A. Definitions

Appendix B. Acronyms

Appendix C. References

Preface

P.1 Purpose

a. This NASA Procedural Requirement (NPR) establishes the Agency-wide personnel security program implementation requirements set forth in NASA Policy Directive (NPD) 1600.2E, NASA Security Policy, as amended.

b. This NPR prescribes personnel security program responsibilities and procedural requirements for the investigation, security clearance determination, continuous evaluation, contractor fitness, adjudication, and appeals of NASA Federal and contractor employees.

P.2 Applicability

a. This NPR is applicable to NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NPR is applicable to all NASA civil service employees, NASA contractor employees, personnel completing work through Space Act Agreements or Memorandums of Agreement (MOA) or Memorandums of Understanding (MOU), those assigned or detailed under the Intergovernmental Personnel Act, partners, recipients of grants and cooperative agreements, and visitors.

c. In this directive, all document citations are the latest version unless otherwise noted.

d. In this NPD, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive materials.

P.3 Authority

a. National Aeronautics and Space Act, as amended, 51 U.S.C. § 20113 (a)

P.4 Applicable Documents and Forms

a. National Security Positions, 5 C.F.R. pt. 732

b. Suitability, 5 C.F.R. pt. 731

c. National Security Information, 32 C.F.R. pt. 2003

d. Suspension and Removal, 5 U.S.C. § 7532

e. Executive Order 10450, Security Requirements for Government Employment, of April 17, 1953, as amended

f. Executive Order 12829, National Industrial Security Program, of January 6, 1995, as amended

g. Executive Order 12968, Access to Classified Information, of August 2, 1999, as amended

h. Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, fitness for contractor employees, and eligibility for Access to Classified National Security Information, of June 30, 2008

i. Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust, of January 22, 2009

j. Executive Order 13526, Classified National Security Information, of December 29, 2009

k. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors of August 27, 2004

l. Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors," March 2006, as amended

m. Office of Personnel Management Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide," dated January 14, 2008

n. Office of Personnel Management Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," dated July 31, 2008

o. White House Memorandum for William Leonard, Director, Information Security Oversight Office, and Subject: Adjudicative Guidelines, Tab A, "Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," dated December 29, 2005

p. Office of Personnel Management Federal Investigations Notice No. 10-05, "Reminder to Agencies of the Standards for Issuing Credentials under HSPD-12," dated May 17, 2010

q. NPD 1440.6H, NASA Records Management

r. NPR 1441.1D, NASA Records Retention Schedules

s. NPR 1600.2A, NASA Classified National Security Information (CNSI)

t. Standard Form SF 50, Notification of Personnel Action

u. Standard Form SF 85, Questionnaire for Non-Sensitive Positions

v. Standard Form SF 85P, Questionnaire for Public Trust Positions

w. Standard Form SF 86, Questionnaire for National Security Positions

x. Standard Form SF 85P-S, Supplemental Questionnaire for Selected Positions

y. Standard Form SF 87, OPM Fingerprint Card

z. Standard Form SF 312, Classified Information Nondisclosure Statement

aa. Standard Form 2018A, Special Access Request Secret Compartmented Information

bb. FD 258, FBI Applicant Fingerprint Card

cc. INV Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations

dd. INV Form 79C, Report of Agency Unfavorable Adjudicative Action on OPM Investigations

ee. Optional Form OF 306, Declaration for Federal Employment

ff. Optional Form OF 8, Position Description

gg. NASA Form 1630, Request for Access to CNSI

hh. NASA Form 1684, Authorization of Credit Release Report

P.5 Measurement/Verification

a. Compliance with this NPR shall be accomplished by Agency-wide application of uniform suitability, security clearance, contractor fitness, and adjudication procedures that foster reciprocity, reduce duplication efforts, and ensure consistent quality standards for adjudication procedures. Measurement of compliance will rely upon objective and modern analytic methods rather than practices that avoid risk.

b. The Office of Protective Services (OPS) audits, conducts functional reviews of the Centers, and conducts spot-checks and inspections to review Center compliance and implementation of this NPR. OPS audits/reviews are conducted at least every three years, or sooner as required to determine compliance with this NPR. The findings of the audits/reviews are provided to the applicable Center Director for resolution no later than 30 days from the completion of the reviews/audits.

P.6 Cancellation

a. NPR 1600.1, NASA Security Program Procedural Requirements, Chapters 2, 3, 4, and Appendixes A, B, C, M, and N, dated, November 3, 2004.

b. NASA Interim Directive (NID) 1600-96, NASA Personnel Security, dated, July 20, 2011.

/S/
Dr. Woodrow Whitlow, Jr.
Associate Administrator, Mission Support Directorate

Chapter 1. Introduction

1.1 Overview

1.1.1 The NASA Administrator is responsible for implementing a comprehensive and effective personnel security program for the Agency. Personnel Security Investigations (PSI) are used to:

a. Evaluate the character and conduct of Government workers for the purpose of making suitability determinations for covered positions and continuous evaluation through reinvestigations of individuals in positions of public trust as required by Executive Order (EO) 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust, and 5 CFR pt. 731, Suitability.

b. Evaluate the character and conduct of contractor workers by making fitness determinations for contractor employment per contractual requirements.

c. Evaluate the character and conduct of Government workers for excepted service or other non-covered positions.

d. Determine the eligibility of Federal employees for national security positions under EO 10450, Security Requirements for Government Employment, the eligibility for a clearance to access classified information under EO 12968, Access to Classified Information; continuous evaluation through reinvestigation of individuals holding clearances; and 5 CFR pt. 732, National Security Positions.

e. Determine the eligibility under Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors," March 2006, as amended, and Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) as mandated in Federal Information Processing Standards (FIPS) Publication 201-1 for access to Federal facilities and federally controlled information systems. Specifics for PIV processing are outlined in FIPS SP 800-79-1 and referenced in Draft NPR 1600.6, NASA Identity and Credential Management.

1.2 Responsibilities

1.2.1 Assistant Administrator, Office of Protective Services (AA, OPS). The AA, OPS shall:

a. Establish and maintain an efficient personnel security program in accordance with Federal standards consistent with current personnel security/fitness policies, procedural requirements, and guidelines as established by the Security Executive Agent, Director of National Intelligence, and the Suitability Executive Agent, Office of Personnel Management (OPM).

b. Establish and maintain the NASA Central Adjudication Facility (CAF). CAF personnel shall be responsible for adjudicating all PSI results to determine a civil service employee's eligibility for initial or continuing access to Classified National Security Information (CNSI).

c. Serve as Agency Advocate for Electronic Questionnaires for Investigation Processing (e-QIP) and be responsible for designing specific policy, program management, and execution of the e-QIP system.

1.2.2 Center Directors shall:

a. Ensure the Center Chief of Security/Center Chief of Protective Services (CCS/CCPS) manages the Center personnel security program in accordance with this NPR.

b. Ensure full Center compliance with the provisions set forth in this chapter.

1.2.3 The CCS/CCPS shall:

a. Designate a Federal civil service employee with a satisfactorily adjudicated PSI on file with OPM to serve in the role of Program Manager in e-QIP. This employee is responsible for administering e-QIP at the Center level and training new e-QIP users.

b. Process and submit all PSI requests to OPM electronically. E-QIP is mandated for use to submit PSIs for civil service and contractor employees to OPM.

c. Ensure that a check of OPM databases such as Personnel Investigations Processing System/Central Verification System (PIPS/CVS) is performed to identify any previous investigation that will serve reciprocally before initiating a PSI. The acceptance of prior determinations will be based on an equivalent investigation and evidence of a favorably adjudicated investigation on the individual.

d. Maintain close coordination with OPM Investigations Service (OPM-IS) and Federal Investigations Processing Service (OPM-FIPS) and process the appropriate requests for PSIs.

e. Ensure adjudications for credentialing are performed by senior personnel security specialists who have been trained in adjudication by an accredited provider.

f. Process security clearance requests for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

g. Notify the NASA CAF of any adverse information regarding any civil service employee at the Center that holds a National Security clearance or assignment to a sensitive position.

h. Require NASA civil service employees granted a security clearance to execute a Classified Information Nondisclosure Statement (SF 312) in accordance with 32 C.F.R. 2003, National Security Information, prior to access to national security information. i. Suspend a civil service employee's clearance access "for cause" based on developed disqualifying adverse information under the Continuous Evaluation Program.

j. Perform an annual review of civil service employee clearance holders and access requirements to ensure Center personnel security clearance needs are properly managed. The CCS/CCPS will develop and implement the appropriate local procedures necessary to ensure the review is conducted.

k. In cooperation with Office of Human Capital Management (OHCM) Resource Specialists, determine the sensitivity designation for national security position for all existing and newly established civil service positions whose duties clearly reflect the requirement for access to CNSI.

l. Refer all employment suitability cases for NASA civil service employees to the appropriate OHCM for review and adjudication upon receipt of the OPM Report of Investigation (ROI).

m. Assist OHCM personnel by conducting local records checks or automated record checks such as the Central Verification System (CVS), to clarify, expand, or mitigate information that has been provided by the investigation provider or a Department of Justice, National Crime Information Center (NCIC) query when requested.

n. Maintain in accordance with the Privacy Act and existing NASA system of records, individual

personnel security files on all investigated personnel. Review applicable reports with officials in the review process who shall make the determination relative to continued access or revocation of access privileges. Security files will contain:

(1) Copies in Center personnel security file of the OPM Case Closing Transmittal, Certification of Investigation, signed e-QIP release sheets, and a signed and dated copy of the OPM Form OF79A for civil service and contractor employees. NASA CAF personnel will maintain copies of the OPM Form OF79A for Federal employees processed for security clearances.

(2) Any adverse information reports on affected contractor or civil service employees.

(3) Copies of concurrence documentation from Office of International and Interagency Relations (OIIR) for any foreign national granted access to classified information.

(4) Signed copies of Classified Information Nondisclosure Agreements Standard Form 312 (SF 312) for NASA civil service employees who have access to Classified National Security Information (CNSI).

1.2.4 The CCS/CCPS shall establish written procedures for the following:

a. Maintaining personnel security electronic files and distribution instructions for the completion of all electronic forms for the investigation process.

b. Assuring the appropriate investigation has been conducted for each NASA Federal or contractor employee.

c. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation if needed to make a credentialing decision.

d. Conducting local records checks or automated records checks when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS/CCPS.

e. Making appropriate notifications for confirmation of the results of a favorable access determination or actions as a result of a non-favorable access determination.

1.2.5 The Center OHCM organizations shall:

a. Ensure that appropriate management and supervisory personnel identify and develop the position descriptions for positions that require access to CNSI. These position descriptions will reflect the level of national security access.

b. Ensure no recruitment, hiring, or change of position action takes place until the appropriate position sensitivity level and risk designation has been established and the position description has been updated to reflect the change.

c. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this chapter.

1.2.6 The Director, OHCM at each Center shall:

a. Designate all covered positions as high, moderate, or low risk as determined by the potential for adverse impact to the efficiency and integrity of the service.

b. Verify employment eligibility of a civil service new hire. Review OPM Form OF 306, Declaration for Federal Employment Form documents for new hires. Review I-9 documents or coordinate the review with CCS/CCPS.

c. Grant reciprocity to prior suitability determinations in accordance with 5 C.F.R. pt 731 or ensure e-QIP is transmitted to OPM on a civil service new hire no later than 14 days after entry on duty (EOD) date.

d. Ensure that supervisors are advised on the proper processing of any personnel who may be reassigned or are the subject of other personnel actions, including termination, resulting from the revocation of security clearance.

1.2.7 Managers and supervisors shall:

a. Ensure full compliance with the requirements established in this policy.

b. Jointly with OHCM, ensure appropriate and accurate position risk designation and sensitivity levels are assigned for all civil service employees under their purview.

c. Assist OHCM personnel during the suitability determination process.

d. Ensure that civil service employees requiring reinvestigation are initiated according to OPM and OHCM position risk and sensitivity levels requirements.

1.2.8 The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NPR.

1.2.9 Contract Management Officials (Contractor Management, Contracting Officer, Contracting Officer's Technical Representative (COTR), and Project Managers) shall:

a. Ensure full compliance with this NPR.

b. Coordinate with the CCS/CCPS for the designation of risk for contractor employees and the timely on boarding of contractor employees.

1.3 Waivers and Exceptions

1.3.1 Centers may occasionally experience difficulty in meeting specific security requirements established by NASA policy. The process for submitting requests for waivers or exceptions to specific elements of the NASA security program requires that the program or project manager and CCS/CCPS justify the waiver request through:

a. Security risk analysis, (e.g., cost of implementation);

b. Effect of potential loss of capability to the Center;

c. Compromise of national security information;

d. Injury or loss of life; loss of one-of-a-kind capability; or

e. Inability of the CCS/CCPS to perform its missions and goals.

(1) Justification will also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

(2) The waiver request shall be submitted to the Center Director.

1.3.2 The Center Director shall either recommend approval or return the waiver request to the CCS/CCPS for further study or closure. The Center Director forwards concurrence to the Mission Support Directorate Associate Administrator.

1.3.3 The Mission Support Directorate Associate Administrator shall forward waiver requests to the AA, OPS requesting concurrence and/or comments or a return of the proposals to the Center director for further study or closure.

1.3.4 The AA, OPS, shall return the waiver request to the Mission Support Directorate Associate Administrator with a recommendation for approval of the waiver, for further study or denial.

1.3.5 The Mission Support Directorate Associate Administrator shall return the waiver requests to the Center Director with concurrence and/or comments or return proposals for further study or closure.

1.4 Violations of Security Requirements

1.4.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA personnel security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. § 799, that provides fines or imprisonment for not more than 1 year, or both.

Chapter 2. NASA Personnel Security Investigations

2.1 General

2.1.1 Individuals who perform work for or on behalf of the Agency are subject to a PSI to determine whether they are:

a. Suitable for Government employment;

b. Eligible for logical and physical access;

c. Eligible for access to classified information;

d. Eligible to hold a sensitive position;

e. Fit to perform work for or on behalf of the Government as a contractor employee.

2.1.2 A determination of both b. and e. applies to all NASA contractors.

2.1.3 An appointment will not be subject to investigation when the person being appointed has undergone a previous PSI and the appointment involves:

a. Appointment or conversion to an appointment in a covered position if the person has been serving the agency for at least one year in a covered position subject to investigation.

b. Transfer to a covered position, provided the person has been serving continuously for at least one year in a covered position subject to investigation.

c. Transfer or appointment from an excepted service position that is not covered to a covered position, provided the person has been serving continuously for at least one year where the person has been determined fit for appointment.

d. Appointment to covered position from a position as an employee working as a Federal Government contract employee provided the person has been serving continuously for at least one year in a job where the Federal agency determined that the contract employee was fit to perform work on the contract.

e. Appointment to a covered position where there has been a break in service of less than 24 months, and the service immediately preceding the break was in a covered position, an excepted service position, or a contract employee position described in paragraphs (a) to (d) of this section.

2.1.4 NASA determines the fitness of contractor employees to perform work as a contractor. Prior favorable fitness, suitability, and national security determinations should be reciprocally accepted. There is no requirement that the prior favorable fitness, suitability, or national security determination be made within a specific time period. However, for contractor employees there should be no break in employment since a favorable determination was made.

2.1.4.1 Contractor employee means an individual who performs work for or on behalf of NASA under a contract and who, in order to perform the work specified under the contract, requires access to space, information, information technology systems, staff, or other assets of NASA. Such contracts include, but are not limited to:

a. Contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the Agency;

b. Sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contracts with the Agency excepted service to the extent they are not otherwise subject to OPM appointing authorities.

2.1.4.2 Non-NASA employees performing work through Cooperative Agreements, Space Act Agreements, Grants, Enhanced Use Lease Agreements, and Funding Orders shall be adjudicated for security access as a contractor consistent with Draft NPR 1600.6, Identity and Credentialing Management.

2.1.4.3 Intergovernmental Personnel Act (IPA) employees may be identified as a civil service employee on the PIV badge. However, the IPA employee would be adjudicated for security access as a contractor.

2.1.5 An appointment to a covered position will also be subject to investigation when:

a. The covered position requires a higher level of investigation than previously conducted for the person being appointed; or

b. The Agency obtains new information in connection with the person's appointment that calls into question the person's suitability.

2.1.6 Federal employees from other Federal Government agencies and members of the U.S. military who are detailed to NASA or who are members of a tenant Federal Government organization are assumed to have been properly adjudicated for employment suitability or fitness to perform work on a Government contract by their respective agency. The CCS/CCPS shall coordinate with the Center OHCM personnel to validate investigative and suitability results for detailees. Upon validation, no further investigation is required unless specifically required by policy or for cause. All subsequent issues associated with personnel identified in this paragraph will be coordinated with the Center OHCM specialists or respective detailee's official agency personnel office for resolution.

2.1.7 Investigations that meet the requirements for a specified position shall be reciprocally accepted for that and lower investigations with no additional investigation provided there is no break in employment, derogatory or questionable information, or need based on change of position with a higher investigation requirement.

2.2 Public Trust Positions

2.2.1 Positions designated at the moderate-risk or high-risk level are referred to as "public trust" positions. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust and involving access to or operation or control of financial or personnel records, with a significant risk for causing damage or realizing personal gain. Public trust positions are subject to periodic reinvestigation.

2.3 Designation of Risk and Sensitivity Levels

2.3.1 Position risk designations and sensitivity levels for civil service employees are made by Center OHCM in coordination with the supervisor and Center Office of Protective Services. This section refers only to non-covered positions.

2.3.2 Position risk and sensitivity level designations for contracts, grants, cooperative agreements, and MOAs or MOUs shall be made by the responsible NASA Center program office representative typically by the designated civil service project manager (sponsor), COTR, in coordination with the CCS/CCPS, and IT Security Manager(s).

2.3.3 The position risk and sensitivity level is determined by evaluating the sensitivity and risk of the work being performed, the access required by the contractor employee, and the potential for damage to NASA's mission and operations if performed inefficiently, ineffectively, or in an unsafe or unethical manner. Included is the requirement to properly identify and assign risk level designations for those individual positions directly involved in IT systems and/or application software development commensurate with the risk and the sensitivity level that will ultimately be applied to the system and or application when deployed.

2.3.4 All access factors (i.e., Center, facility, information, and IT systems) will be considered concurrently as part of the overall risk designation process. This procedure serves to avoid duplication of effort by eliminating the possibility that a single individual could be assessed numerous times for different accesses. The intended result will be that the highest level of risk designation is the designation for which the appropriate investigation will be conducted (IT = high-risk designated position compared against that same individual's need to access uncontrolled areas of the Center = low-risk) .

2.3.5 The risk and sensitivity level for each position shall be identified and designated in the statement of work of the contract. This position designation determines the investigative requirements for the contractor employees that perform the work.

2.3.6 Fitness determinations will be made for contractor employees upon consideration of contractual requirements.

2.3.7 If an employee's duties require any overlap into a higher or lower risk level, the position risk will then be set at the highest risk level anticipated.

2.3.7.1 The COTR in consultation with the contracting officer is required to identify the employees to be processed at each risk level designation and will specify the duties of the contractors. In instances where there is a wide variance in the security risk level of the work to be performed, individual contractor employees will be processed at the risk designation commensurate with the highest risk level of their duties.

2.3.7.2 The entire contract, grant, MOA, or MOU may be designated high or moderate risk, but those NASA contractor employees whose work would be moderate or low risk will be investigated accordingly. In meeting this contingency, the contract, grant, MOA, or MOU will specifically apply controls to ensure that work of the lower risk positions does not overlap with that for the higher risk positions.

2.4 High-Risk Public Trust Positions

2.4.1 High-risk positions are those that have the potential for exceptionally serious impact involving duties especially critical to the Agency or a program mission of the Agency with a broad scope of policy or program authority.

2.5 Moderate-Risk Public Trust Positions

2.5.1 Moderate-risk positions are those that have the potential for moderate-to-serious impact

involving duties of considerable importance to the Agency or a program mission of the Agency with significant program responsibilities and delivery of customer services to the public.

2.6 Low-Risk Positions

2.6.1 Low-risk positions are those that have the potential for limited impact involving duties of minimal relation to the Agency mission with program responsibilities that affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a high-risk or moderate-risk position. Positions designated at the low-risk level are not considered public trust positions.

2.6.2 Positions that do not fall in the categories high-risk or moderate-risk include all non-sensitive positions and all other positions involving IT Systems whose misuse has limited potential for adverse impact or sensitive data is protected with password and encryption. Low- risk IT positions may involve general word processing or systems containing no IT-1 or IT-2 level information.

2.6.3 The contractor program manager and COTR will identify and specify control measures to be used to ensure that there is no overlap of work duties between the lower designated positions.

2.6.4 Non-U.S. citizens, including Lawful Permanent Residents, are eligible for placement in low-risk and moderate-risk positions, but are not normally eligible for employment in positions designated as high-risk. Under specific situations the AA, OPS may authorize the placement of a non-U.S. citizen for a specific high-risk position when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization should submit a written request to the AA, OPS, via the CCS/CCPS. The request should contain the following:

a. Specify why it is impractical or unreasonable to use U.S. citizens to perform the required work or function.

b. Define the individual's special expertise.

c. Define the compelling reasons for the request.

2.6.5 The CCS/CCPS will review the request for accuracy, endorse or non-endorse it, and forward it to the AA, OPS.

2.6.6 The AA, OPS, will coordinate with OIIR for concurrence, and if approved, promptly return the request to the requestor. A copy will be retained in OPS and Center security office files.

2.7 Child Care Providers

2.7.1 Child Care National Agency Check and Inquiries (CNACI) are to be completed on all child care providers prior to their working in NASA-sponsored child care facilities. Centers shall use the services of OPM to conduct these investigations.

2.7.2 Upon return of favorable OPM fingerprint results and severe operational need, personnel shall work under regular and continuous observation by a favorably adjudicated employee, pending completion of the CNACI on the observed individual.

2.7.3 NASA child care centers shall coordinate all personnel hiring actions with the Center security office prior to entry on duty.

2.8 Lautenberg Amendment

2.8.1 Federal and contractor employees in positions that require the carrying of a firearm are affected by the Lautenberg Amendment to the Gun Control Act of 1968, effective September 30, 1996. The amendment makes it a felony for those convicted of misdemeanor crimes of domestic violence to ship, transport, possess, or receive firearms or ammunition. The amendment also makes it a felony to transfer a firearm or ammunition to an individual known or reasonably believed to have a conviction.

2.9 Personnel Security Investigations Requested by NASA

2.9.1 NASA will comply with OPM standards for requesting PSIs. Security offices will use the following chart to select the appropriate investigation:

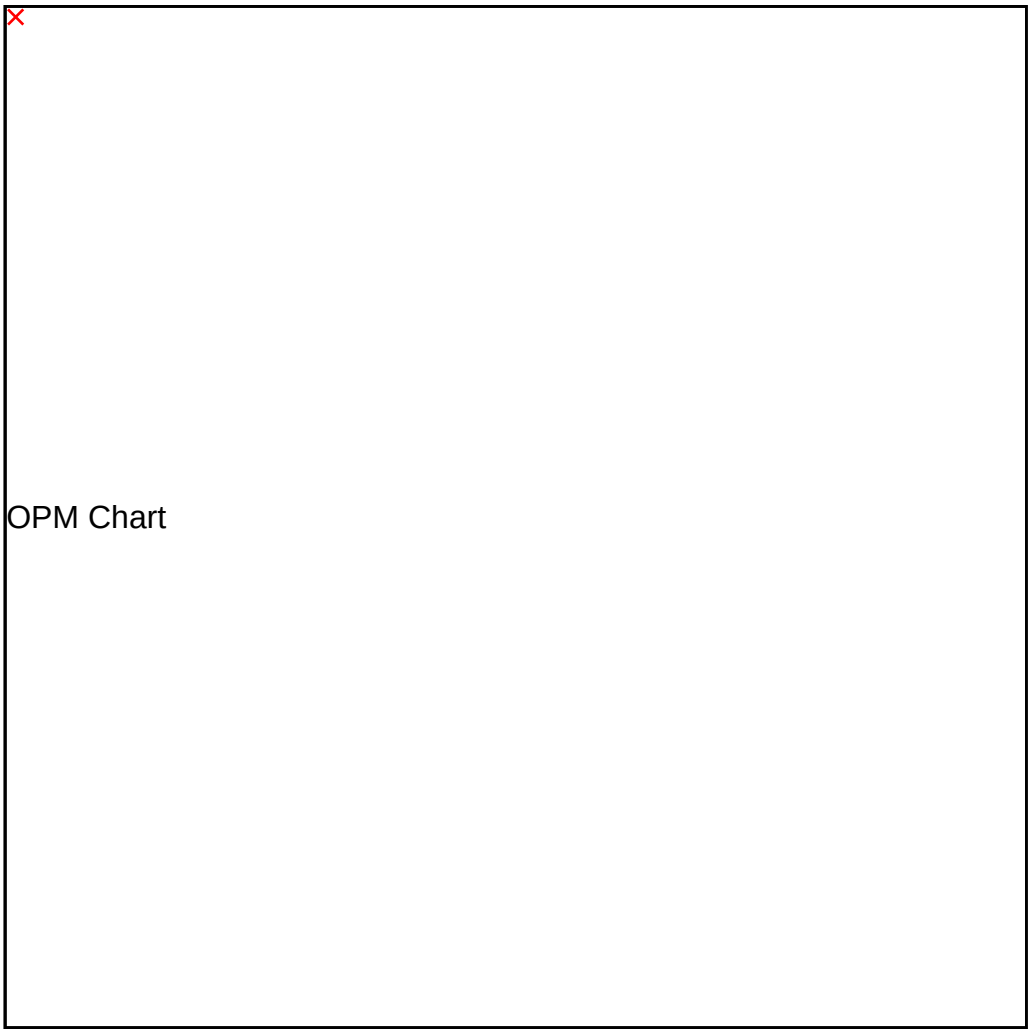

Figure 1, OPM Chart

2.9.2 If the required investigation is determined not to have been accomplished during a routine audit or review for an employee, or as mandated by changes in regulations by OPM, the CCS/CCPS will ensure the appropriate investigation is conducted as follows:

a. The NASA program sponsoring the employee shall provide the NASA security office with the necessary funding to accomplish the required investigations.

b. The sponsor shall notify OHCM personnel for civil service employees and the CCS/CCPS for contractor employees and whether a PSI will be initiated for the employee in e-QIP if required.

c. The employee shall submit to fingerprinting, complete and submit the electronic forms in e-QIP, and sign the appropriate release pages.

2.9.3 The timing of security form submittal and the established risk level may dictate whether a proposed NASA employee can begin work prior to a final access determination. The CCS/CCPS shall advise the sponsor whether the individual can commence working prior to the receipt of the completed investigation and final access determination based on the specifics of the situation and a preliminary review of the fingerprint card results and submitted forms.

2.10 Investigation and Reinvestigation Requirements for NASA Civil Service Employees and Appointees without Access to CNSI

2.10.1 Center OHCM offices shall initiate a NACI in e-QIP on a SF 85 for new civil service employees and appointees performing duties in low-risk positions. Initial investigations require the employee to complete the SF 85, an OF 306, and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87. Center security offices may initiate any investigation type in e-QIPs on behalf of OHCM upon approval of the CCS/CCPS.

a. Center security offices shall initiate a reinvestigation for low-risk civil service employees and appointees every ten years in e-QIP utilizing the NACI investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85 and submit to fingerprinting upon notification by the security office.

2.10.2 Center OHCM offices shall initiate a Moderate Background Investigation (MBI) in e-QIP on a SF 85P for new, transferred or promoted civil service employees and appointees performing duties in moderate-risk public trust positions. Initial MBI investigations require the employee to complete the SF 85P, an OF 306 and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87.

a. Center security offices shall initiate a reinvestigation for moderate-risk public trust civil service employees and appointees every five years in e-QIP utilizing the NACLC investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85P and submit to fingerprinting upon notification by the security office of reinvestigation.

2.10.3 Center OHCM offices shall initiate a Background Investigation (BI) in e-QIP on a SF 85P for new, transferred or promoted civil service applicants and appointees performing duties in high-risk public trust positions. Initial BI investigations require the employee to complete the SF 85P, an OF 306 and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87.

a. Center security offices shall initiate a reinvestigation for high-risk public trust civil service employees and appointees every five years in e-QIP utilizing the Periodic Reinvestigation (PRI) investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85P and submit to fingerprinting upon notification by the security office of reinvestigation.

2.10.4 When a civil service employee or appointee experiences a change in duties due to promotion or reassignment and the risk level is higher, a new investigation commensurate to the risk should be transmitted to OPM within 14 calendar days of the effective date of the action.

2.11 Investigation and Reinvestigation Requirements for NASA Contractor Employees without Access to CNSI

2.11.1 Center security offices shall initiate an NACI in e-QIP on a SF 85 for contractor employees performing duties in low-risk positions. Investigations requested on the SF 85 also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on a FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor low-risk reinvestigations shall be initiated every ten years utilizing the NACI investigative product from OPM. The contractor employee will electronically complete a SF 85 and submit to fingerprinting upon notification by the security office of reinvestigation.

2.11.2 Center security offices shall initiate an MBI in e-QIP on a SF 85P for contractor employees performing duties in moderate-risk public trust positions with no access to CNSI. Investigations requested on the SF 85P also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on an FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor moderate-risk public trust reinvestigations shall be initiated every five years utilizing the NACLC investigative product from OPM. The contractor employee will electronically complete the SF 85P in e-QIP and submit to fingerprinting upon notification by the security office of reinvestigation.

2.11.3 Center security offices shall initiate a BI in e-QIP on a SF85P for contractor employees performing duties in high-risk public trust positions with no access to CNSI. Investigations requested on the SF 85P also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on an FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor high-risk public trust reinvestigations shall be initiated every five years in e-QIP utilizing the Periodic Reinvestigation (PRI) investigative product from OPM. The contractor employee will electronically complete an SF 85P in e-QIP and submit to fingerprinting upon notification by the security office of reinvestigation

2.11.4 When a contractor employee experiences a change in work due to promotion or reassignment and the risk level is higher, a new investigation commensurate to the risk should be transmitted to OPM within 14 calendar days of the effective date of the action.

2.12 Processing Personnel Security Investigation Requests in e-QIP

2.12.1 Electronic Questionnaires for Investigation Processing (e-QIP) is a secure Web site that is designed to transmit all PSI requests. The questionnaires processed through e-QIP include: SF 85, Questionnaire for Non-Sensitive Positions; SF 85P, Questionnaire for Public Trust Positions; and SF 86, Questionnaire for National Security Positions.

2.12.2 Every e-QIP user, both Agency staff and applicant, has specific responsibilities that correspond to e-QIP roles as follows:

a. Agency Advocate: The highest-level official within each activity. This role is the AA, OPS.

b. Agency Administrator: OPM-FIS's main point of contact at the Agency for e-QIP. This position is located in OPS' Security Management Division.

c. Technical Administrators: The experts in technology available at each Agency and the Agency

Chief Information Officer (CIO).

d. User Administrator: Enters Agency users into e-QIP based upon duties and level of investigation of staff working in e-QIP. e. Program Manager: Serves as the day-to-day point of contact for initiators, reviewers, and approvers at each Center. f. Business Manager: User role with access to the View Reports option in e-QIP responsible for generating standard reports based on e-QIP data such as the Agency request status, Agency user role, and Agency request event count reports. g. Approver: Conducts a final review of the investigation and forwards the request to the Investigation Service Provider (ISP). The e-QIP approver shall be a Federal employee.

h. Reviewer: Examines the investigation request and forwards it to the approver, if applicable.

i. Initiator: Serves as the applicant's main point of contact during the investigation request process.

j. Agency Help Desk: Able to reset Golden Questions for applicants who have active requests in their agency or within a subordinate agency and view an applicant's request summary.

2.12.3 OPM has mandated that individuals who are given roles in e-QIP are vetted as follows:

a. Agency administrator, program manager, approver, and reviewer role: NACLC or MBI.

b. User administrator: SSBI or BI.

c. Business managers, initiators, and agency help desk: NACI.

2.12.4 E-QIP users should access the OPM portal as a gateway to the e-QIP database. The portal is a secure, encrypted environment known as the OPM's Investigative Service (OPMIS) secure portal. The OPMIS secure portal can be used for the exchange of Sensitive but Unclassified Information (SBU), such as Privacy Act Information and Personally Identifiable Information (PII). E-QIP users and other community members with portal access can send and receive email, review and download documents, and access information on OPM products and services through the portal. In addition to e-QIP, the portal acts as the gateway to OPM-Federal Investigative Services Division (FISD) computer systems, such as Personnel Investigations Processing System (PIPS) and CVS. E-QIP users who do not use their e-QIP role assignments within a 35-day period will be deactivated from access to OPM's secure portal.

2.12.5 E-QIP Approvers must be Federal employees. They are responsible for properly annotating the appropriate Security Office Identifier (SOI) to ensure the completed SF 86s are returned by OPM to the NASA CAF for adjudication. This SOI number is available from NASA CAF personnel.

2.13 Individuals with Prior Criminal Record

2.13.1 Individuals with a criminal record (except minor traffic) shall be adjudicated for access in accordance with Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," July 31, 2008, and "Memorandum to Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, Security Clearance Decision Making Guide" January 14, 2008.

2.14 Adverse Information

2.14.1 When adverse information is self-reported, developed or received in the course of any personnel security investigation, or subsequent to such investigation and initial favorable

determination, the scope of inquiry shall be expanded to the extent necessary to obtain sufficient information to make a reasonable and sound determination as to whether the employee is fit to perform work for or on behalf of the Government and/or is eligible for logical and physical access.

2.14.1.1 These expanded inquiries shall be conducted by a NASA security or OHCM official with appropriate investigative experience, NASA contracted investigators, by the original investigating agency, or by another agency of the Federal Government at NASA's request.

2.14.1.2 Any expanded investigation may consist of many different lines of inquiry including, but not limited to, interviews of the employee, supervisors, co-workers, neighbors, and physicians; records checks with various local agencies; and credit checks.

2.14.2.1 Appropriate signed releases from the employee shall be obtained when required to pursue additional leads such as medical records and credit checks.

2.14.2.2 Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center Counterintelligence Office.

2.14.3.1 A personal interview or expanded inquiry shall be held with an employee on whom significant unfavorable or derogatory information has been developed or received during the screening process. The employee shall be offered an opportunity to refute, explain, clarify, or mitigate the information in question.

2.14.3.2 The personal interview or expanded inquiries shall be conducted by a qualified NASA security official, by the original investigating agency, or another agency of the Federal Government at NASA's request.

2.14.4 Agency officials shall conduct a new fitness determination at any time adverse information is obtained that calls into question an individual's fitness based on character or conduct. This may include a new PSI or database query and adjudication. Adverse information involving civil service employees shall be referred to the Center OHCM for appropriate action.

2.15 Reciprocity of Other Agency Adjudications

2.15.1 OPM's CVS shall be checked by a NASA trusted information provider who has undergone a favorably adjudicated PSI to determine if a prior investigation will serve reciprocally for a NASA determination for contractor fitness or access to physical and logical resources. If there is no favorably adjudicated PSI identified in CVS or any other trusted government agency that will serve reciprocally, a PSI will be initiated in e-QIP for the contractor employee commensurate to the risk level associated with the contract.

2.15.2 Reciprocal recognition of fitness shall be granted for a prior favorable fitness or suitability determination when:

a. Equivalent 5 C.F.R. Pt. 731 adjudicative criteria was used for Federal employees and OPM's Final Credentialing Standards for issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008, was used for contractor employees; and

b. The individual has had no break in employment since the favorable determination was made. With regard to contractor employees, a break in employment also refers to a break in employment on a Federal contract, and not just a break in employment with a particular contractor. If the individual has stopped working on a Federal contract, but continues to work for the contractor on a non-Federal contract, this is deemed to be a break in employment.

2.15.3 NASA personnel are not required to grant reciprocal recognition for a prior favorable fitness or suitability determination when:

a. The new position requires a higher level of investigation than previously conducted for that individual; or

b. An agency obtains new information that calls into question the individual's fitness based on character or conduct; or

c. The individual's investigative record reflects conduct that is incompatible with the core duties of the new position; or

d. The investigation is out of scope.

2.16 HSPD-12 Credentialing Standards

2.16.1 OPM's Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," July 31, 2008, shall be used by trained adjudicators to determine eligibility for physical and logical access only. PIV authorizers will be trained in adjudication by certified adjudication training providers if they perform adjudication duties. A PIV card will not be issued to a person if:

(1) The individual is known to be or reasonably suspected of being a terrorist;

(2) The employer is unable to verify the individual's claimed identity;

(3) There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;

(4) There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

(5) There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or

(6) There is a reasonable basis to believe the individual will use federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

2.16.2 When a person does not require a suitability determination or a security clearance, adjudicators shall apply seven Supplemental Credentialing Standards. These standards are intended to ensure that the grant of a PIV card to an individual does not create an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; records; or to the privacy of data subjects. A PIV card will not be issued to a person if:

(1) There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;

(2) There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

(3) There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a

PIV card poses an unacceptable risk;

(4) There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(5) There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(6) A statutory or regulatory bar prevents the individual's contract employment or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or

(7) The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

2.16.3 For the purpose of this adjudicative policy, the "whole person concept" is defined for those eligible for physical and logical access. Logical and physical access shall be granted for individuals on whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicate there is no unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial or medical records; or to the privacy of data. An individual's trustworthiness, honesty, reliability, discretion, and sound judgment are fundamental to the adjudicative process. This "whole person concept" will provide a balanced assessment of positive as well as negative aspects of an individual's past and present activities.

2.16.4 Adjudicators will use the OPM's Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide," dated January 14, 2008, as a resource for deriving a reasonable conclusion or decision based on the standards outlined in OPM's Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD -12."

2.16.4.1 Adjudicators will not add or delete or modify the adjudicative standards. Final adjudications for suitability will be performed within 90 days from receipt of a ROI from OPM.

2.16.4.2 The investigation closing date and adjudicative action will be recorded in IdMAX, submitted on OPM form INV 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations or electronically annotated in OPM PIPS/CVS under Agency Menu as soon as possible after adjudication. Flat files from IdMAX may also be uploaded into OPM's PIPS/CVS system.

2.17 Reconsideration Procedures for Contractor Employees and other Agency Affiliates

2.17.1 Notice of Proposed Action - When an adjudicator determines that a PIV applicant has not provided his or her true identity, the applicant is determined unfit for Center access or to be employed in the current or applied for position based on an unfavorable adjudication, the adjudicator shall provide the individual reasonable notice of the determination including the reasons(s). The notice should state the specific reasons for the determination and that the individual has the right to answer the notice in writing within 10 working days. The notice will inform the individual of the

time limits, as well as the address to which the response should be made.

2.17.2 The individual may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

2.17.3 Decision - After consideration of any documentation submitted by the PIV applicant for reconsideration of the initial determination, the CCS/CCPS or his/her designee will issue a written decision (usually within 10 days), which informs the PIV applicant of the reasons for the favorable or unfavorable decision.

2.17.4 Reconsideration - If a denial letter is provided and the PIV applicant subsequently requests an appeal, the Center Director shall appoint a Credentialing Adjudication Review Panel (CARP) to review the information surrounding the denial of access. The panel will be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members shall have a favorable PSI and only one of the panel members may be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the CARP or they may request to appeal in person to the CARP. Any approved personal appearance before the CARP will be documented by means of a written summary or recording which will be made a part of the applicant's security record.

2.17.5 Prior to finalizing the CARP determination, a CARP panel member or the CCS/ CCPS may refer the CARP proposed decision to the Center Director for an additional level of review. If no referral is made to the Center Director, the CARP decision is final. If there is a referral to the Center Director, the Director's decision is final.

2.17.6 Upon determination that a denial has been upheld, there is no further reconsideration process. The individual may be debarred from access to the NASA Center, based on the denial for a period of one to three years. The IdMAX shall reflect any debarments to the Center, based on denial or revocation of PIV.

2.18 Personnel Security File Storage and Access

2.18.1 Records and information related to this policy shall be managed in accordance with NPD 1440.6H, NASA Records Management, and NPR 1441.1D, NASA Records Retention Schedules. Personnel security files are temporary records and are destroyed in accordance with the disposition instructions NPR 1441.1D.

2.18.2 Information from personnel security files may be disclosed to a Federal agency in response to requests in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation, the classifying of a position, the reporting of an investigation of an employee, the letting of a contract, and/or the issuance of a license, grant, or other benefit by the requesting agency to the extent that the information is appropriate for release to the requesting official, relevant and necessary to the requesting agency's decision on the matter.

2.18.3 Subjects of personnel security investigations and screenings may request copies of excerpts, summaries, or any analytical extract of information from the NASA case file under the Freedom of Information Act and Privacy Act procedures. The subject may not be provided a copy of any third-party investigations (i.e., OPM, FBI). The subject should obtain copies of the third-party investigation directly from the appropriate agency.

2.18.4 The results of OPM PSIs are furnished to NASA for the limited purpose of making suitability, security, and/or fitness determinations. E-delivery investigations adjudicative actions shall be reported using the "Enter Agency Adjudication" function on the Personnel Investigations Processing System (PIPS) Agency menu, which is accessible through either a dedicated PIPS terminal or OPM FIS' Web-based Secure Portal. E-delivery information processors/users shall destroy the distributed investigative file after eligibility has been rendered and/or the data is no longer needed.

a. Requests for an OPM investigative file for any other purpose should be directed to OPM. Requests should be referred to OPM and not to a NASA Center security office. OPM's investigative files are maintained in a Privacy Act System of Records; therefore, OPM must determine if there is a statutory provision or a published routine use that permits them to release the investigative file without an individual's written authorization.

2.18.5 OPM's FISD maintains the PIPS, a system which maintains the Security/Suitability Investigations Index (SII). The SII is a repository of millions of PSI records of Federal employees, contract employees, and military personnel. These records are maintained for a minimum of 16 years. NASA Security Specialists who are authorized by the OPS Director, Security Management Division may access these files and perform searches of the database to determine if an individual already has a PSI that may serve for hiring, credentialing, or granting a security clearance. Authorized individuals can perform SII searches, request files, and transmit messages to OPM as well as access security clearance information and HSPD-12 credentialing information through the CVS.

2.18.6 Center security office personnel shall securely maintain personnel security investigative and screening records for credentialing decisions on all NASA civil service and contractor personnel. Center security offices may use databases maintained by OHCM to confirm the position risk and sensitivity of civil service employees rather than maintaining duplicative file copies of position descriptions. These records can be stored electronically at the discretion of the CCS/CCPS at each Center as long as the information technology system allows for encryption at rest of PII. However, Center security offices should be able to convert the documents into an accessible, reproducible, legible, quality approved electronic format. Once the conversion has been completed, the contents of the document may be recognized as the official record. Paper documents such as PSIs, investigation scheduling notices, and advance National Agency Checks (NACs) that have served their purpose and are no longer needed may be destroyed via shredding or burning.

Chapter 3. Personnel Security Investigations for National Security Positions

3.1 General

3.1.1 National security requires each agency to follow established procedures to identify national security positions. Positions identified by this process within NASA require regular use of or access to classified information, or to occupy a sensitive position. This chapter addresses the sensitivity designation program associated with national security, the criteria for determining national security sensitivity levels, and investigation type screenings.

3.1.2 Position sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a national security position, could cause to national security.

3.1.3 Investigations are conducted to provide a basis for ensuring that the granting of a security clearance to an individual is clearly consistent with the interests of national security.

3.1.4 Personnel security reports and records shall be handled in accordance with the Privacy Act of 1974.

3.1.5 OPM conducts a range of investigations that satisfy the various requirements for the three position-sensitivity levels described in this chapter, as they relate to accessing CNSI.

3.1.6 NASA contracts requiring the generation of and/or access to CNSI shall be processed in accordance with the requirements of EO 12829, the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

3.2 Scope

3.2.1 This chapter prescribes the procedures whereby NASA Federal employees are selected, processed, investigated, and adjudicated for national security positions, consistent with adjudicative guidelines contained in White House Memorandum, Adjudicative Guidelines, dated, December 29, 2005, and the OPM's Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide.

3.2.2 This chapter applies to contractor employees providing services under a NASA classified contract that requires access to Sensitive Compartmented Information (SCI).

3.3 Program Oversight

As part of its responsibility for the functional management and oversight of the NASA Personnel Security Program, OPS shall verify compliance with personnel security clearance requirements when conducting functional reviews or periodic audits of Center security programs.

3.4 Principles of Personnel Security Clearance Management

3.4.1 The purpose of the personnel security clearance program is to ensure that only loyal,

trustworthy, and reliable people are granted access to classified information or assigned to sensitive duties.

3.4.2 Due to the cost and time invested in conducting the appropriate investigation, managers and supervisors should be judicious and accurate in determining an employee's position sensitivity and need for access to CNSI. Managers and supervisors should establish the access requirement during the development of the individual position description and assign the appropriate designation of position risk and sensitivity level for each NASA position description. Failure to properly identify upfront the need for access to CNSI causes added expense that will be borne by the program and results in unnecessary delays.

a. Managers and supervisors should discuss with the employee their responsibilities and obligations in handling CNSI prior to initiating a new PSI for access to CNSI.

3.4.3 The requirement for access to CNSI shall be clearly established during submission of the NF 1630, Request for Access to CNSI and the position description development phase. Once the position has been determined to require access to CNSI and position sensitivity has been assigned, the new appointee must complete the SF 86 in e-QIP.

3.4.4 Access to CNSI shall not be requested or granted solely to permit entry to, or ease of movement within NASA controlled areas, other Government agency facilities, or contractor facilities when the individual involved has no need for access to classified information.

3.4.5 Requests for security clearances shall not be processed or granted based merely on a speculative need for access or as a result of any particular grade, position, or affiliation. Requesting security clearances for contingency purposes in excess of actual official requirements is prohibited.

3.4.6 The level at which access to CNSI is requested and granted shall be clearly documented on the NF 1630, Request for Access to Classified National Security. Access to CNSI must be limited and should relate directly to the level of classified information for which access is clearly justified in the performance of official duties and for which the individual has a demonstrated "need to know."

3.4.7 PSI and eligibility determination shall be mutually and reciprocally accepted by all agencies unless an agency has substantial information indicating an employee may not satisfy the access eligibility standards.

a. Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations. They may also be reinvestigated at any time, if there is reason to believe that they may no longer meet the standards for access.

3.4.8 A person may have access to classified information provided that:

a. A favorable determination of eligibility for access has been made by an agency head or the agency head's designee; and

b. The person has executed an SF 312; and

c. The person has a need-to-know the information.

3.4.9 The Center security office will notify the employee in writing when an interim or final clearance eligibility decision has been made, or a reciprocal clearance has been accepted. The Center security office shall conduct all required orientation training as well as ensure the execution, witness, acceptance, and storage of the SF 312 consistent with 32 C.F.R. pt. 2003.20, Classified Information Nondisclosure Agreement: SF 312.

3.4.10 Every person who has met the standards for access to classified information will receive

training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

3.4.11 An annual review of clearance and access requirements is necessary to ensure Center personnel security clearance needs are properly managed. The CCS/CCPS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

3.4.12 Personnel with clearances who have not had the need to access CNSI during the previous year will be given serious consideration for administrative withdrawal of their clearance as determined by supervisors during the revalidation process.

3.4.13 Clearances will not be retained merely as a stop-gap measure in the event the holder may need access to CNSI. A clear demonstrable operational requirement is necessary to possess the clearance as annotated in the position description.

3.4.14 Results of the favorable adjudication determination will be posted and made available to Center security personnel via the NASA Clearance Tracking System (NCTS).

3.5 Sensitive Compartmented Information (SCI)

3.5.1 Candidates for SCI access shall have a favorably adjudicated Top Secret (TS) investigation.

3.5.2 Requests for access to SCI require the submittal of Form 2018A, Special Access Request Form.

3.5.3 The Form 2018A shall be prepared and justified by the employee's immediate supervisor. The line supervisor will submit it through the division director, or higher, depending on the applicant's organizational position, for review and approval. The request is then forwarded along with a copy of the employee's updated SF 86 to the HQ Special Security Office (SSO) for appropriate action. 3.5.4 A copy of the Form 2018A and the original signed SCI Non-Disclosure Form shall be retained by the SSO representative at the Center.

3.5.5 PSIs for access to classified information for individuals requiring TS, SCI, or Q (Department of Energy Restricted Data) clearance access are subject to periodic reinvestigations at any time following the completion of, but no later than five years from the date of, the previous investigation.

3.6 One-Time Access Determinations

3.6.1 Urgent operational requirements may occur where a NASA Federal employee in a non-sensitive position has a one-time or short duration requirement for access to CNSI at the Confidential or Secret level. Usually, the limited duration or nature of this access requirement does not warrant processing the individual for a personnel security investigation and final security clearance eligibility determination. One-time access determinations will not be granted for the TS level. One-time access determinations will be used sparingly and only under conditions of compelling Government need. CCS/CCPS or an official designated by the CCS/CCPS has the authority to grant one-time access determinations subject to the following terms and conditions.

3.6.2 One-time access determinations should not be issued more than three times to any person within a one calendar year time frame. The aggregate access will not exceed a total of 60 days accumulated during a single calendar year.

3.6.3 One-time access determinations shall only be granted to U.S. citizens that have been

continuously employed by the Federal Government for the preceding 24 months.

3.6.4 If the need for access is expected to exceed 60 days, the individual will be processed for a final security clearance determination.

3.6.5 An individual requiring one-time access will complete a NASA Form 1630, Request for Access to CNSI, and have at least a favorable National Agency Check and Inquiries, or a criminal history and credit check with a favorable suitability determination and local records check. Such individuals will complete an SF 86 for review by a trained adjudicator.

3.6.6 An individual requiring one-time access to CNSI will execute an SF 312. The SF 312 shall be witnessed, accepted, and stored as required in Section 3.4.9 of this NPR.

3.6.7 One-time access determinations, subsequent debriefs, and any security clearance certification (i.e., one-time clearance granted from date-to-date) shall be properly documented in local Center security office files. NCTS shall not be used to document one-time access determinations.

3.7 Coding of Position Sensitivity Level Designation for National Security Positions

3.7.1 National security positions are designated as non-critical sensitive, critical sensitive, or special sensitive.

3.7.2 The proper coding of position sensitivity for national security positions is required on Position Description OF 8 and optional on the Notification of Personnel Action SF 50.

3.7.3 Center OHCM personnel are responsible for managing the Electronic Position Description System (e-PDS). They will coordinate in a timely manner with managers, supervisors, and the CCS/CCPS to accomplish sensitivity designation of positions for individuals requiring access to CNSI. After the appropriate position sensitivity determination has been assigned, the Center OHCM or OPS personnel will initiate the appropriate investigation in e-QIP.

3.7.3.1 Individuals in positions designated low risk that may have access to classified information will be vetted at the level commensurate with the clearance requirements. For example, a custodian serving in a position designated as low risk who works in an area with classified information would be processed on a SF 86 for an Access National Agency Check and Inquiries (ANACI) rather than a SF 85 or SF 85P to meet the appropriate scope of the investigation in support the clearance required. Guidance for designating position sensitivity levels is contained in Chapter 2.9 of this NPR.

3.7.4 SPECIAL-SENSITIVE (SS): Positions requiring access to Top Secret Sensitive Compartmented Information (TS/SCI) shall be designated Special-Sensitive and the individual will undergo a SSBI using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access to TS/SCI.

3.7.4.1 Pre-appointment investigation requirements shall not be waived for positions designated SS.

3.7.5 SPECIAL ACCESS PROGRAM (SAP): Access to SAP information requires a current favorably adjudicated PSI for the appropriate classified level prior to being granted access to the information. National SAP requirements dictate that periodic reinvestigation shall be conducted every five years for all SAP personnel.

3.7.6 CRITICAL-SENSITIVE (CS): Positions requiring access to Top Secret (TS) or North Atlantic Treaty Organization (NATO) information will be designated critical-sensitive. Individuals in or selected for these positions shall undergo a SSBI, using SF-86, and be favorably adjudicated prior to

being granted access to information.

3.7.7 NONCRITICAL-SENSITIVE (NCS): Positions requiring access to Secret, Confidential, or NATO Secret/Confidential information shall be designated noncritical-sensitive. New hires selected for these positions will undergo, at a minimum, an ANACI, using SF-86 in e-QIP, and be favorably adjudicated prior to being granted access to information.

3.7.8 Pre-appointment waivers from Center Human Resources Directors may be authorized by the AA, OPS to approve an emergency appointment or reassignment to a CS or NCS position prior to completion of the required pre-appointment investigation only when clear justification exists to warrant the waiver.

3.7.9 NON-SENSITIVE: Non-sensitive positions relate to any position that is not a national security position.

3.7.10 All NASA positions designated as testing designated positions (TDP) will be in accordance with EO 12564. Personnel holding active security clearances shall be entered into the Drug Testing Program for random testing.

3.8 Temporary/Interim Access to Classified National Security Information (CNSI)

3.8.1 Management officials are required to request temporary access eligibility for U.S. citizen employees, civil service employees, and/or consultants filling CS and NCS positions when essential and immediate operational requirements do not allow for waiting for a pending personnel security investigation to be completed and adjudicated.

3.8.2 Center security offices shall document requests and approvals for temporary access eligibility and will provide compelling justification to warrant access to CNSI in advance of formal investigation and adjudication. In all cases, the required personnel security investigation will be initiated, entered into NCTS, transmitted to OPM, and have a favorable NAC results prior to issuance of the interim Secret and Confidential clearance. All interim TS clearance requests shall be submitted to the AA, OPS, for approval.

3.9 Access to CNSI by Non-U.S. Citizens

3.9.1 Non-U.S. citizens (including lawful permanent residents (LPR)) are not eligible for a security clearance. However, under specific situations the AA, OPS, may authorize the granting of a Limited Access Authorization (LAA) to a non-U.S. citizen for specific information up to the Secret level when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization shall submit a written request to the AA, OPS, via the CCS/CCPS. The request should:

a. Specify why it is impractical or unreasonable to use U.S. citizens to perform the required work or function.

b. Define the individual's special expertise.

c. Define the compelling reasons for the request.

d. Explain how access will be limited and physical custody of CNSI precluded.

e. Request concurrence or non-concurrence and forward it to the AA, OPS.

3.9.2. The AA, OPS, will coordinate with the Office of International and Intergovernmental Relations (OIIR) for concurrence and if approved, return it to the requestor. A copy shall be retained in the OPS CAF and CCS/CCPS files. The CCS/CCPS shall ensure:

a. A completed investigation and favorable adjudication is obtained before access is granted. The granting of interim or temporary access pending the completion of an investigation is prohibited.

b. Denied requests shall be returned to the requestor with an explanation of the denial.

c. Individuals with LAAs will be placed under closely controlled supervision of appropriately cleared persons (U.S. citizens). Managers will be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

d. Individuals who have been granted an LAA shall not be allowed access to any classified information other than that specifically authorized under national disclosure policy. Additionally, physical custody of classified information by these individuals is not authorized.

e. Non-U.S. citizens are ineligible for access to intelligence information, communications security keying materials, TS information, Restricted or Formerly Restricted Data, Critical Nuclear Weapons Design Information (CNWDI), TEMPEST information, classified cryptographic information, or NATO classified information.

f. Requests for access to CNSI owned by another agency must be coordinated with and approved by that agency.

3.9.3 Access to classified information will be limited to that necessary to complete the task, and access shall be terminated upon completion of the task.

3.9.4 If the access request is initiated by a NASA-cleared contractor performing on a NASA classified contract, only the Defense Industrial Security Clearance Office (DISCO) or successor organization has the authority to grant access to a LAA to non-U.S. citizens. Procedures for coordination of the request are as follows:

a. A cleared contractor's Facility Security Officer will receive the endorsement of the CCS/CCPS, Center International Visitor Coordinator (IVC), Center Export Administrator (CEA), OIIR, and AA, OPS.

b. The CCS/CCPS will ensure the contract is current and evaluate the justification for the request. The non-U.S. citizen nominated for the LAA will sign a nondisclosure statement executed by the CCS/CCPS. The CCS/CCPS shall forward the completed package to the AA, OPS, for review, coordination, and endorsement.

c. If acceptable, the AA, OPS, shall endorse and return it to the contractor for forwarding to the DISCO. A completed SSBI and favorable adjudication is required before access is granted.

d. Denied requests shall be returned to the contractor with an explanation of the denial.

3.10 Reciprocal Recognition of Security Clearance Determinations

3.10.1 Acceptance of access eligibility determinations will be implemented in the following manner:

a. An employee with an existing security clearance (not including an interim clearance) who transfers or changes employment status is eligible for a security clearance at the same or lower level

without additional or duplicative adjudication, investigation, or reinvestigation and without any requirement to complete or update a security questionnaire unless substantial information exists indicates that the standards may not be satisfied.

3.10.2 The "substantial information" exception to reciprocity recognition of security clearances does not authorize NASA personnel to request a new security questionnaire, review existing PSI questionnaires, or initiate new investigative checks (such as a credit check) to determine whether such substantial information exists.

3.10.3 Prior investigations shall be accepted reciprocally, provided the following conditions are met:

a. There has been no break in service in excess of 24 months; and

b. The prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position; and

c. There has been no subsequent development of potentially disqualifying derogatory information.

3.10.4 Reciprocity will not be granted if the following conditions apply:

a. The individual has more than 24 months break in service; or

b. A favorable adjudication is more than five years old; or

c. The agency obtains new information that calls into question the individual's continued eligibility for access to CNSI.

3.11 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)

3.11.1 Access to Restricted Data (RD) and Formerly Restricted Data (FRD) outside the scope of aeronautical and space activities require clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC).

3.11.2 If such access is required solely for the performance of service for another agency, that agency normally shall initiate the required investigation. In such a case, the OPM reimbursable investigation required for the occupant of a sensitive position will not be initiated.

3.11.3 The Central Adjudication Facility (CAF) shall assist the other agency by obtaining and providing the required security documents.

3.11.4 When access to RD or FRD outside the scope of aeronautical and space activities are required in the performance of NASA duties, a request for either a DOE or an NRC clearance shall be initiated by the CCS/CCPS, who will forward the necessary documents to the Special Security Officer for appropriate action.

3.12 Guiding Principles for Adjudication, Suspension, Denial, or Revocation of Security Clearances

3.12.1 The Adjudicative Guidelines for Determining Eligibility for Access to Classified Information serve as a guide for investigators and adjudicators to identify potential issues that may adversely affect an individual's eligibility for access to classified information.

3.12.2 Only the AA, OPS, or his designee shall deny or revoke a security clearance.

3.12.3 The AA, OPS, and CCS/CCPS may suspend security clearances.

3.12.4 Adjudications shall be fully documented and recorded in the subject's security file and entered into the NASA Clearance Tracking System (NCTS).

3.12.5 Information developed during the investigation process for a security clearance may not be shared with the Center OHCM or management while the investigation is pending. The AA, OPS or CCS/CCPS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, is a threat to a critical mission, or shall otherwise be ineligible for or lose continuation of Federal employment.

3.12.6 All reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

3.12.7 The CCS/CCPS will propose suspensions of security clearances to the NASA CAF for cause based on developed adverse information. The AA, OPS, will make final denial or revocation determinations after consultation with the NASA CAF and Office of General Counsel personnel.

3.12.8 Requests for a security clearance shall result in an adjudicative determination unless, unrelated to any potential adjudication factor, the need for the security clearance no longer exists, such as severance of the subject's employment.

3.12.9 Subjects of adjudication are allowed to refute any information developed during the investigation process that may make the person ineligible for access to classified information.

3.12.10 In the event of a denial or revocation of a security clearance, the subject is entitled to obtain a review of the decision.

3.12.11 Center OHCM personnel, in coordination with security office personnel and supervisors, will make employment suitability determinations. The Center OHCM shall coordinate and document those determinations. They are separate and distinct from security clearance adjudications.

3.12.12 The policies and the procedures for the suspension, denial, and revocation of a security clearance shall not be confused with the procedures for the removal of an employee on national security grounds as set forth in 5 U.S.C. § 7532, Suspension and Removal. A CCS/CCPS may coordinate with OHCM to pursue the removal of an employee on national security grounds, regardless of the sensitivity of the employee's position or whether the employee has access to classified information.

3.13 Bond Amendment

3.13.1 The Bond Amendment 50 U.S.C. § 435c (b) repealed the Smith Amendment 10 U.S.C. § 996, and places restrictions that are similar to the Smith Amendment, but which apply to all Federal Government agencies. The Bond Amendment bars persons from holding a security clearance for access to Special Access Programs, Restricted Data, and SCI if they have been:

a. Convicted of a crime and served more than one year of incarceration.

b. Discharged from the Armed Forces under dishonorable conditions.

c. Determined to be mentally incompetent by a court or administrative agency.

3.13.2 The Bond Amendment also prohibits all Federal agencies from granting or renewing a security clearance for any covered person who is an unlawful user of controlled substance(s) or is an

addict; this prohibition applies to all clearance holders.

3.14 Adjudication of Security Clearances

3.14.1 The AA, OPS, and the NASA CAF adjudicators are empowered to determine an employee's security clearance eligibility.

3.14.2 Each investigation required for a specific clearance level will be complete with sufficient scope in order to appropriately adjudicate for access to classified information.

3.14.3 In instances when management, for reasons unrelated to the adjudicative process, withdraws a request for a security clearance and the subject of the investigation continues his or her employment with NASA, potential issue information developed during the investigative process will be made available to OHCM to make a suitability determinations.

3.14.4 The initial adjudication will be made once the adjudicator has gathered all available pertinent information.

3.14.5 The senior adjudicator shall review the initial adjudication for fairness, completion, and proper application of the adjudication guidelines.

3.15 Suspension of Security Clearances

3.15.1 The AA, OPS, Center Director, or the CCS/CCPS shall suspend an individual's security clearance when information is developed that suggests the individual's continued access to classified information is not in the interest of national security. The determination to suspend should be based on thorough review of definitive derogatory information. All suspensions will be reported immediately to the Central Adjudication Facility by way of the NASA Clearance Tracking System.

a. The subject shall be notified accordingly. However, the reason or reasons for a suspension need not be provided to the subject of a suspension.

b. Suspension of a security clearance shall not be open-ended. Every effort should be expended to complete the investigation and to adjudicate as soon as practical. All suspension actions should be resolved as soon as practical from the date of the suspension.

c. Suspension of an individual's access to classified information is not an adverse action. Suspension merely allows the agency time to investigate and adjudicate information that may affect the individual's eligibility for access to classified information.

d. A suspension is a temporary status. The subject of a suspension is not entitled to the review procedures required for denial or revocation of a security clearance.

e. Upon receipt of suspension information containing documented facts that fully support the suspension, CAF personnel will determine whether to reinstate or revoke the clearance of the individual.

3.16 Denial or Revocation of Security Clearances

3.16.1 No individual will be given access to classified information or assigned to a sensitive position unless a favorable security eligibility determination has been made. In the event of an unfavorable adjudication action, the NASA CAF shall propose documented reasons in a Letter of Intent (LOI) to

deny or revoke a clearance.

3.16.2 The Director, Security Management Division (DSMD) shall review the proposed unfavorable adjudicative action by CAF personnel and:

a. Remand the case for further work; or

b. Uphold the proposed adjudication of the information, and in consultation with the Office of General Counsel, provide written notice to the subject of the denial of the revocation of the security clearance through the CCS/CCPS.

3.16.3 The employee shall acknowledge receipt of the LOI and determine whether he/she intends to respond within the time specified in the LOI. If the subject provides new information for consideration, CAF personnel shall review the new information provided. CAF personnel will make a recommendation to the DSMD whether a security clearance should be reinstated, revoked, or denied. If inadequate or no information is provided or no response is provided within the specified time allowed, CAF personnel will continue with the denial or revocation process. Upon completion of the process, the subject will be notified by the DSMD of a final decision in a Letter of Notification (LON). The letter is served through the CCS/CCPS.

3.16.4 If the subject receives a LON of denial or revocation, the subject will be afforded an opportunity to appeal the LON to the AA, OPS.

3.16.5 The AA, OPS, shall ensure that the rights of the subject are protected and due process is accorded, including the opportunity for the subject to appear in person to present relevant documents, materials, and information prior to final determination by the AA, OPS. If the employee takes advantage of the opportunity to appear personally before the AA, OPS, the AA, OPS will document such appearance by means of a written summary or recording which will be made a part of the subject's security record.

3.16.6 If the AA, OPS, provides a notice of denial or revocation and the subject subsequently requests an appeal by a Security Adjudication Review Panel (SARP), the NASA Administrator will appoint that body. The panel will be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members will have a favorable SSBI, and only one of the panel members may be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the SARP or they may choose to appeal in person to the SARP. Any personal appearance before the SARP will be documented by means of a written summary or recording which will be made a part of the subject's security record.

3.16.7 Prior to finalizing the SARP determination, a SARP panel member or the AA, OPS, may refer the SARP proposed decision to the Administrator for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If there is a referral to the Administrator, the Administrator's decision is final.

3.16.8 Upon determination that a clearance revocation or denial has been upheld, the case then becomes one of employment suitability and shall be referred to OHCM for suitability determination.

3.17 Continuous Evaluation of Security Clearance Eligibility

3.17.1 A personnel security clearance determination is based on a continuous assessment of an individual's personal and professional history, demonstrated loyalty to the United States, strength of character, trustworthiness, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential coercion and willingness to abide by regulations governing the

use, handling, and protection of CNSI.

3.17.2 In order to ensure that all persons who have been granted a security clearance remain eligible, all U.S. Government clearance holders shall be subject to a continuous evaluation of their qualifications to meet the high standards of conduct expected of persons in national security positions.

3.17.3 Persons subject to a prior favorable personnel security determination who demonstrate behavior that places doubt on their loyalty, reliability, or trustworthiness or otherwise disqualifies that individual for continued eligibility for a security clearance shall be subject to further scrutiny and possible suspension of access to CNSI.

3.17.4 Center Directors and the CCS/CCPS shall ensure that a program of continuous evaluation for security clearance eligibility is developed that relies on all levels of management and all security clearance holders to be aware of the standards of conduct for qualification to hold a security clearance and their responsibility to report adverse behavior that is disqualifying. Where employees have significant involvement with handling, storing, marking, or exercising original or derivative classification of CNSI, supervisors will include these responsibilities as a critical element of the employees' annual performance communication system documentation.

3.17.5 Supervisors and managers are critical to the success of the Continuous Evaluation Program. Supervisors shall report incidents of potentially disqualifying behavior that they are aware of to the CCS/CCPS and be observant to potential changes in behavior of their subordinates that could cause potential risk to the CNSI to which the employee has been entrusted.

3.17.6 Holders of security clearances and other employees with knowledge that an employee holds a security clearance shall be advised and periodically reminded to report to their supervisor or appropriate security officials when they become involved in behavior or become aware of such behavior of another cleared individual that could impact their continued eligibility for access to CNSI. A security clearance holder who fails to report disqualifying conduct involving other cleared personnel is also subject to suspension of access to CNSI, pending a security inquiry.

3.17.7 CCS/CCPS should conduct fact finding of reports of disqualifying conduct, and depending on the adverse impact to national security, may suspend an individual's access to CNSI for cause. CCS/CCPS may request a periodic assessment or other PSI to support their assessment of the employees' continued access to classified information. CCS/CCPS will forward a report to the NASA CAF personnel as soon as possible after fact finding. CAF personnel will determine if the individual continues to be eligible for access to CNSI.

3.18 Classified Visits and Meetings

3.18.1 Classified visits to other agencies. Employees who have a need to certify their security clearance should contact their Center security office.

a. An inter-agency clearance verification request can be generated by the security office upon review of the NCTS and then forwarded to the facility or custodian.

b. The request may be completed by the personnel security specialist or special security officer who has access to NCTS.

c. Visit requests are normally issued for no more than one year at a time. Visit requests for longer than one-year are at the discretion of the agency being visited. A copy shall be maintained in the security file for record.

3.18.2 Classified visit requests and classified meetings. Employees hosting meetings involving classified information will advise the prospective attendees to have their agency security office prepare and transmit certifications of the attendees' security clearances to the respective Center personnel security office or the special security officer. The certifications should include the investigation record information used as a basis to grant the clearance, Center point of contact, purpose, and duration of the visit. If these certifications are not forwarded, then custodians of the classified materials may verify the clearances of attendee's in OPM's PIPS/CVS system. Clearances from agencies that cannot be verified in the PIPS/CVS system will require a certification of clearance from the agency.

3.18.3 Special Access Program (SAP) Visits. All visit requests involving special access programs shall be processed by the appropriate special security office.

Appendix A. Definitions

Access - The ability, opportunity, and authority to gain knowledge of classified information or gain authorized entry onto a NASA classified IT resource.

Adjudication - A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, ability to perform work for or on behalf of the Government as a contractor employee or access to NASA facilities, information, or IT resources, is in the best interest of national security or efficiency of the Government.

Asset - A system, object, person, or any combination thereof that has importance or value; which includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Automated Record Checks (ARC) - A centralized and integrated set of IT services to request, collect, and validate electronically accessible, adjudicative-relevant data using the most efficient and cost-effective technology and methods available. ARC's are a lawfully acceptable replacement of legacy and non-automated record checks. Ultimately, ARC entails fully automatic machine-to-machine interaction to request, collect, and validate machine-readable data and inform subsequent steps in an end-to-end electronic case management system.

Center Chief of Security/Center Chief of Protective Services (CCS/CCPS) - The senior security official at a Center that is responsible for technical management of the Center security program.

Central Adjudication Facility (CAF) - Facility established at the OPS Security Management Division level responsible for adjudicating all requests for clearances to access CNSI.

Certification - A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Classified Material - Any physical object on which is recorded, or in which is embodied, CNSI that shall be discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information (CNSI) - Information that is protected against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cohabitant - An individual with whom the applicant resides in a spouse-like relationship.

Compromise - The improper or unauthorized disclosure of or access to classified information.

Continuous Evaluation - Reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial and Government databases and other lawfully available information) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information

Contractor Employee - For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA IT; an expert or consultant to any agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors, a personal services contractor, or any other category of person who performs work for or on behalf of any agency (but not a Federal employee). In order to perform the work specified

under the contract, will require access to space, information, IT systems, staff, or assets of NASA.

Core Duty - means a continuing responsibility that is of a particular importance to the relevant covered position or the achievement of an agency's mission.

Corroborate - Comparing information from any investigative source with that provided by the subject to confirm the information or identify discrepancies.

Covered Individual - A person who performs work for or on behalf of the executive branch, or seeks to perform work for or on behalf of the executive branch, but does not include the President or Vice President.

Covered Positions - These positions are as follows: position in the competitive service; positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and career appointments to positions in the Senior Executive Service.

Credential - A Personal Identity Verification Card issued to an individual that contains stored biometric information so that the claimed identity of the cardholder can be verified against the stored information manually or by an automated process.

Critical Sensitive (CS) - One of the three levels for designating national security-related positions and the degree of risk involved. Includes any position involving access to Top Secret information; investigative requirements for this position are covered under National Security Directive 61.

Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

Denial - The adjudication that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in Executive Order 12968 have been exercised.

Electronic Questionnaires for Investigation Processing System (e-QIP) - A Web-based tool for self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct investigations.

Enhanced Subject Interview - An in-depth discussion between a trained and certified investigator and the subject conducted as a required part of an investigation or to offer the subject an opportunity to explain, refute, or mitigate issue or discrepant information.

Excepted Service - those positions: (a) not in the competitive service, (b) not in the Career Senior Executive Service, and (c) not in the intelligence community unless covered by OPM appointing authorities.

Executive Order - Official documents, numbered consecutively, through which the President of the United States manages the operation of the Federal Government.

Federally Controlled Facility - has meaning prescribed in guidance pursuant to the Federal Information Security Management Act.

Fitness - The level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee

Fitness Determination - A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than in an excepted service position subject to

suitability) or as a contractor employee.

Foreign National - For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States including lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee status to the United States. See definition of Lawful Permanent Resident (LPR) in this chapter.

Formerly Restricted Data (FRD) - Information developed by the Department of Energy (DOE) related to national nuclear programs with strict access restrictions, "Restricted Data (RD)," but that has subsequently been downgraded to a lower level of control and accountability.

Immediate Family - The spouse, parents, siblings, children, and cohabitant of the subject. This includes any stepparents, half siblings and stepsiblings, and stepchildren of the subject.

Information Technology System (ITS) - An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Intelligence Community - The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services; the Federal Bureau of Investigation; the Department of Homeland Security; the Department of the Treasury; the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

Intergovernmental Personnel Act (IPA) - Individuals on temporary assignments between Federal agencies and state, local, and Indian Tribal Governments, institutions of higher education, and other eligible organizations.

Investigative Record - The official record of all data obtained on the subject from trusted information providers from suitability and/or security applications and questionnaires and any investigative activity conducted under Federal standards.

Lawful Permanent Resident (LPR) - Replaces the term "Permanent Resident Alien (PRA)" - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). LPRs are afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector except for specific needs or under temporary appointments. (NOTE: LPRs are not prohibited from accessing export controlled commodities, but must still have a work related "need-to-know" and are still considered foreign nationals under immigration laws. LPRs shall be vetted, for credentials, exactly like a U.S. citizen.)

Logical Access - Access to federally controlled information systems and data.

NASA Employee - NASA civil service personnel.

National Security Positions - Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

a. Confidential - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the Original Classification Authority (OCA) is able to identify or describe.

b. Secret - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the OCA is able to identify or describe.

c. Top Secret - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

Nondisclosure Agreement - Standard Form 312 (SF 312) is a non-disclosure agreement required under EO 13292 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the Information Security Oversight Office of the National Archives and Records Administration and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. The SF 312 replaces the earlier forms SF 189 or the SF 189-A. Enforcement of SF-312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion, or removal, in addition to the likely loss of the security clearance."

Periodic Reinvestigation (PRI) - The PRI consists of a National Agency Check, a credit search, a personal subject interview, selected record searches (for example, law enforcement, personnel security files, and official personnel files (OPF)). Coverage is for a 7-year period. A PRI is required for all high-risk positions.

Permanent Resident Alien (PRA) - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). PRA's shall be afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments), and access to CNSI. (NOTE: PRA's are not prohibited from accessing export controlled commodities, but must still have a work related "need-to-know" and are still considered foreign nationals under immigration laws. PRAs shall be vetted, for credentials, exactly like a U.S. citizen.)

Physical Access - Access to federally controlled facilities, other than on an occasion or intermittent basis.

Position Risk Designation - The assessment of the potential for adverse impact on the efficiency and integrity of the service and the degree to which, by the nature of the position, the occupant could bring about a material adverse effect on the national security.

Position Sensitivity - The designation of the level of risk associated with a position based on the actual or possible access to CNSI.

Public Trust Position - Position at the high-risk or moderate-risk level would normally be designated as public trust positions. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities or other duties demanding a significant degree of public trust, and positions involving access to or operation or control of financial records with a significant risk for causing damage or realizing personal gain.

Reciprocity - The reciprocal recognition of suitability or fitness determinations is intended to simplify and streamline investigative and adjudicative processes where prior determinations are based on equivalent investigations and adjudicative criteria. Reciprocity limits the need to conduct a new fitness determination when an individual moves without a break in employment from a position in the Federal Government to an excepted service or contractor position or from a contractor position to an excepted service position or another contractor employee position.

Revocation - The removal of an individual's eligibility to access classified information based upon an adjudication that continued access to classified information poses a risk to national security and

after review procedures.

Risk Acceptance - An official acknowledgement by management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate a risk.

Risk Assessment - The process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

Risk Management - A means for NASA management to implement select measures designed to reduce or mitigate known risks.

Security Clearance - A designation identifying an individual's highest level of allowable access to classified information, based upon a positive adjudication that the individual does not pose a risk to national security.

Security Violation - an act or action by an individual or individuals that is in conflict with NASA security policy or procedure such as a loss or compromise of CNSI, refusal to properly display NASA Photo-ID, violation of escort policy, or security area violations. (NOTE: Does not include incidents of criminal activity, theft, assault, DUI, and others.)

Senior Management Official - Agency or Center management personnel at Division Chief or higher level.

Sensitive Compartmented Information (SCI) - Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

Special Access Program (SAP) - Any program established and approved under Executive Order 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Suitability - Refers to identifiable character traits and past conduct which are sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of a Federal job. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

Suspension - The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

Trusted Information Provider - An authorized individual working for or on behalf of the Government who may contact references or otherwise corroborates or verifies subject data, such as citizenship, education, and former employment. These individuals may include Government and contract employees or military personnel, working in human resources or security offices, or equivalent organizations.

Unauthorized Disclosure - A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

Verification - Validating at the actual source (an individual or place of record - such as employers, courts, law enforcement agencies - or their authorized repositories) the correctness and accuracy of information listed on the e-QIP/e-Application or provided by the subject or references to the trusted information provider.

Waiver - The approved continuance of a condition or process authorized by the AA, OPS, that varies

from a mandatory requirement and implements risk management on the designated vulnerability being waived.

Appendix B. Acronyms

AA	Assistant Administrator
ANACI	Access National Agency Check and Inquiries
ARC	Automated Records Check
BI	Background Investigation
CAF	Central Adjudication Facility
CARP	Credentialing Adjudication Review Panel
CCS	Center Chief of Security
CEA	Center Export Administrator
CEP	Continuous Evaluation Program
CNACI	Child Care National Agency Check and Inquiries
CNSI	Classified National Security Information
COTR	Contracting Officer's Technical Representative
CCPS	Center Chief of Protective Services
CCS	Center Chief of Security
CNWDI	Critical Nuclear Weapons Design Information
CS	Critical Sensitive
CVS	Central Verification System
DAA	Designated Approving Authority
DISCO	Defense Industrial Security Clearance Office
DOE	Department of Energy
EO	Executive Order
EOD	Entry on Duty Date
E-QIP	Electronic Questionnaires for Investigation Processing
FISD	Federal Investigative Services Division (OPM)
FRD	Formerly Restricted Data
IPA	Intergovernmental Personnel Act
HSPD	Homeland Security Presidential Directive

ITAR	International Traffic in Arms Regulation
ITS	Information Technology System
IVC	International Visitor Coordinator
LAA	Limited Access Authorization
LOI	Letter of Intent
LON	Letter of Notice
LPR	Lawful Permanent Resident
MBI	Moderate Risk Background Investigation
MEI	Mission Essential Infrastructure (replaced by NCI-NASA Critical Infrastructure)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NACLC	National Agency Check with Law and Credit
NCI	NASA Critical Infrastructure (formerly, MEI- Mission Essential Infrastructure)
NCIC	National Crime Information Center (DOJ)
NCTS	NASA Clearance Tracking System
NPD	NASA Policy Directive
NRC	Nuclear Regulatory Commission
NPR	NASA Procedural Requirement
NSD	National Security Directive
OCA	Original Classification Authority
OGC	Office of General Counsel
OHCM	Office of Human Capital Management
OIIR	Office of International and Interagency Relations
OPF	Official Personnel File
OPM	Office of Personnel Management
OPMIS	Office of Personnel Management's Investigative Service

OPS	Office of Protective Services
PII	Personally Identifiable Information
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PPO	Program Protection Office
PRA	Permanent Resident Alien
PRI	Periodic Reinvestigation
PSI	Personnel Security Investigation (formerly Background Investigation)
RD	Restricted Data
ROI	Report of Investigation
SAP	Special Access Program
SARP	Security Adjudication Review Panel
SCI	Sensitive Compartmented Information
SF	Standard Form
SII	Security/Suitability Investigations Index
SMD	Director, Security Management Division
SSBI	Single Scope Background Investigation
TDP	Testing Designated Position

Appendix C: References

C.1 Unlawful Acts, 18 USC §922 (g) (9), Lautenberg Amendment

C.2 Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. §799

C.3 Security Clearances; Limitations, 50 U.S.C. §435c (b)

C.4 Executive Order 10450, Security Requirements for Government Employment of April 27, 1953

C.5 Executive Order 12564, Drug-free Federal workplace of September 15, 1986

C.6 Executive Order 12829, National Industrial Security Program, as amended

C.7 Executive Order 13292 - Further Amendment to Executive Order 12958, as Amended, Classified National Security Information

C.8 OMB Memorandum M-05-24, Memorandum for the Heads of All Departments and Agencies, "Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005

C.9 OMB Memorandum M-11-11, Memorandum for the Heads of Executive Departments and Agencies, "Continued Implementation of Homeland Security Presidential Directive (HSPD) - 12, Policy for a Common Identification Standard for Federal Employees and Contractors," February 3, 2011

C.10 OMB Memorandum for Deputies of Executive Department and Agencies "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2008

C.11Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors of August 27, 2004

C.12 Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors," March 2006, as amended

C.13 Security Executive Agent, Suitability Executive Agent, Memorandum, Approval of Federal Investigative Standards, December 13, 2008

C.14 Memorandum for Heads of Agencies Aligning OPM Investigative Levels with Reform Concepts, August 24, 2010

C.15 Crime Control Act of 1990, Child Care Worker Employee Background Checks, Pub. L. No. 101-647

C.16 e-Gov Act of 2002, Pub. L. No. 107-347, 44 U.S.C. CH. 36

C.17 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec 17, 2004)

C.18 Privacy Act of 1974, Pub. L. No. 93-579

C.19 NPR 1382.1, NASA Privacy Procedural Requirements

C.20 NPR 1600.6, Identity, Credential and Access Management, (NID 1600-95)

C.21 NPR 2810A, Security of Information Technology